

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

Підп. та дата	
Інв. № дубл	
Взам. інв. №	
Підп. та дата	
Інв. № ориг.	

Центр сертифікації ключів ринку електричної енергії

Комплексна система захисту інформації

План захисту інформації

ЄААД.468244.185.Д3.01

2014 р.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ	3
ТЕРМІНИ ТА ВИЗНАЧЕННЯ	3
1 ЗАГАЛЬНІ ПОЛОЖЕННЯ	4
2 НОРМАТИВНІ ПОСИЛАННЯ	4
3 ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЦСК.....	5
4 КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЄТЬСЯ В ЦСК.....	6
5 ОПИС КОМПОНЕНТІВ ЦСК ТА ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ	7
6 ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЇ В ЦСК	7
7 ОСНОВНІ ПОЛОЖЕННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ В ЦСК.....	8
8 ПОЛОЖЕННЯ ПРО ЗАХИСТ ІНФОРМАЦІЇ ЦСК.....	10
9 ПОРЯДОК ПЕРЕГЛЯДУ ПЛАНУ ЗАХИСТУ	12
10 ВІДПОВІДАЛЬНІ ЗА РЕАЛІЗАЦІЮ ПЛАНУ ЗАХИСТУ	12
11 КАЛЕНДАРНИЙ ПЛАН РОБІТ З ЗАХИСТУ ІНФОРМАЦІЇ В ЦСК.....	13
12 СИСТЕМА ДОКУМЕНТІВ З ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЦСК	15
13 ПОРЯДОК ДІЙ У РАЗІ ВІДМОВИ КСЗІ ЧИ ОКРЕМОГО КОМПОНЕНТА.....	16
14 ВИКОНАННЯ РОБІТ, ПОВ'ЯЗАНИХ З ТЕХНІЧНИМ ОБСЛУГОВУВАННЯМ	16
ДОДАТОК 1. ПЕРЕЛІК НОРМАТИВНИХ, РОЗПОРЯДЧИХ, ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ ТА ІНШИХ ДОКУМЕНТІВ, ЗГІДНО З ЯКИМИ ПОВИНЕН ЗДІЙСНЮВАТИСЯ ЗАХИСТ ІНФОРМАЦІЇ В ЦСК.....	17
ДОДАТОК 2. ОПИС КОМПОНЕНТІВ ЦСК ТА ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ	18

ПЕРЕЛІК СКОРОЧЕНЬ

БД	- База даних
ДСТУ	- Державний стандарт України
ЄСКД	- Єдина система конструкторської документації
ЄСПД	- Єдина система програмної документації
ЕЦП	- Електронний цифровий підпис
ІзОД	- Інформація з обмеженим доступом
КЗЗ	- Комплекс засобів захисту
КСЗІ	- Комплексна система захисту інформації
НД	- Нормативний документ
НСД	- Несанкціонований доступ
ОС	- Операційна система
ПЗ	- Програмне забезпечення
ПТК	- Програмно-технічний комплекс
СЗІ	- Служба захисту інформації
ТЗІ	- Технічний захист інформації
ЦСК	- Центр сертифікації ключів

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

У цьому документі використовуються терміни та визначення згідно з:

- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення;
- НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- Правила посиленої сертифікації. Затверджені наказом ДСТСЗІ СБ України № 50 від 10.05.2006 р;
- Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису. Затверджене наказом ДСТСЗІ СБ України №31 від 30.04.04 р. Зареєстроване в Міністерстві юстиції України за №592/9191 від 12.05.04 р;
- Закону України “Про електронний цифровий підпис” від 22.05.03 р;
- Закону України “Про електронні документи та електронний документообіг” від 22.05.03р.

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. План захисту інформації в ЦСК (далі - план захисту) є організаційно-розпорядчим документом, згідно з яким здійснюється організація захисту інформації на всіх етапах життєвого циклу ЦСК.

1.2 План захисту розроблений на підставі проведеного аналізу технології обробки інформації, аналізу ризиків, сформульованої концепції й політики безпеки інформації. План захисту визначає і документально закріплює об'єкт захисту інформації в ЦСК, основні завдання захисту, загальні правила обробки інформації в ЦСК, мету побудови та функціонування КСЗІ, заходи з захисту інформації від несанкціонованого доступу, а також незаконного втручання в процес її обробки.

1.3 Документ не регламентує питання охорони приміщень і забезпечення збереження і фізичної цілісності компонентів ЦСК, захисту від стихійного лиха (пожеж, потопів), збоїв і відмов технічних засобів, збоїв в системі енергопостачання і питання відновлення даних, а також заходи забезпечення особистої безпеки персоналу.

1.4 Вимоги цього документа поширюються на ЦСК в цілому.

1.6 План захисту фіксує на певний момент часу склад ЦСК, перелік оброблюваних відомостей, технологію обробки інформації, склад комплексу засобів захисту інформації, склад необхідної документації та ін. План захисту повинен регулярно переглядатися та при необхідності змінюватись. Зміни та доповнення до плану захисту затверджуються на тому ж рівні та в тому ж порядку, що і основний документ.

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому документі наведено посилання на нормативні документи, перелік яких наведений у дод. 1.

3 ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЦСК

3.1. Основною метою, на досягнення якої направлені всі положення даного документа, є захист власника ЦСК ринку електричної енергії та користувачів ЦСК від можливого нанесення ним матеріального, морального або іншого збитку в наслідок випадкового або навмисного несанкціонованого втручання в процес функціонування ЦСК або несанкціонованого доступу до інформації і її незаконного використання.

3.2. Вказана мета досягається за допомогою забезпечення і постійної підтримки наступних властивостей інформації:

- конфіденційності інформації з обмеженим доступом (ІзОД) у процесі обробки в ЦСК;
- цілісності інформації в процесі обробки в ЦСК та передачі по каналах зв'язку;
- доступності інформації (стійкого функціонування ЦСК, при якому користувачі системи отримують необхідну їм інформацію і результати рішення задач за прийнятний час).

3.3 Завданнями захисту інформації в ЦСК є:

- забезпечення визначених політикою безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації ЦСК;
- своєчасне виявлення та знешкодження загроз для ресурсів ЦСК, причин та умов, які спричиняють (можуть привести до) порушення його функціонування та розвитку;
- створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні ЦСК;
- ефективне знешкодження (попередження) загроз для ресурсів ЦСК шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;
- керування засобами захисту інформації, керування доступом користувачів до ресурсів ЦСК, контроль за їхньою роботою з боку персоналу служби захисту інформації, оперативне сповіщення про спроби НСД до ресурсів ЦСК;
- реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації.

3.4 Рішення завдань захисту інформації в ЦСК досягається:

- регламентацією процесів обробки даних із застосуванням засобів автоматизації й дій співробітників ЦСК, що експлуатують ЦСК, а також дій персоналу, що здійснює обслуговування й модифікацію програмних і технічних засобів ЦСК, на основі затверджених керівництвом ЦСК організаційно-розпорядчих документів з питань забезпечення інформаційної безпеки;
- повнотою охоплення всіх аспектів проблеми, погодженістю і виконанням вимог організаційно-розпорядчих документів з питань забезпечення інформаційної безпеки в ЦСК;
- призначенням і підготовкою посадових осіб (співробітників), відповідальних за організацію й здійснення практичних заходів щодо забезпечення безпеки інформації й процесів її обробки;
- наділенням кожного співробітника ЦСК (користувача) мінімально необхідними для виконання їм своїх функціональних обов'язків повноваженнями по доступу до ресурсів ЦСК;
- чітким знанням і дотриманням всіма співробітниками, що експлуатують і обслуговують апаратні й програмні засоби ЦСК, встановлених вимог з питань забезпечення безпеки інформації;
- персональною відповідальністю кожного співробітника ЦСК за свої дії;
- обліком всіх ресурсів системи (інформації, робочих станцій, серверів тощо);
- застосуванням ефективних заходів забезпечення фізичної цілісності технічних засобів і безперервною підтримкою необхідного рівня захищеності компонентів ЦСК;
- застосуванням фізичних і технічних (програмно-апаратних) засобів захисту ресурсів системи й безперервною адміністративною підтримкою їхнього використання;
- проведенням роботи з персоналом (підбір, роз'яснення, навчання тощо) і ефективним контролем за дотриманням співробітниками ЦСК - користувачами ЦСК вимог з забезпечення інформаційної безпеки;
- юридичним захистом інтересів ДП "ЕНЕРГОРИНОК" при взаємодії підрозділів ЦСК із зовнішніми організаціями (пов'язаному з обміном інформацією) від протиправних дій як з боку цих організацій, так і від несанкціонованих дій обслуговуючого персоналу та третіх осіб;
- проведенням постійного аналізу ефективності й достатності вжитих заходів і застосовуваних засобів захисту інформації, розробкою й реалізацією пропозицій по вдосконаленню системи захисту ЦСК.

4 КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЄТЬСЯ В ЦСК

4.1 Види інформації. За типом її представлення в ЦСК інформаційне забезпечення ПТК ЦСК включає внутрішньомашинну інформаційну базу та позамашинну інформаційну базу.

4.1.1 Внутрішньомашинна інформаційна база являє собою сукупність баз даних і масивів інформації, які обробляються і зберігаються в ПТК ЦСК, а також технологічна інформація КЗЗ і технологічна інформація щодо управління та адміністрування компонентів ПТК ЦСК.

4.1.2 До технологічної інформації КЗЗ належить інформація щодо реєстраційних записів користувачів, їх повноважень та прав доступу до об'єктів, встановлених робочих параметрів (конфігурації) окремих компонентів або засобів захисту, інформація баз даних захисту, інформація журналів реєстрації дій користувачів ПТК ЦСК тощо. Технологічна інформація КЗЗ призначена для використання тільки уповноваженими адміністраторами, технічним обслуговуючим персоналом, що забезпечує функціонування ПТК ЦСК.

4.1.3 До технологічної інформації управління компонентами ПТК ЦСК належить інформація про параметри компонентів технічних та програмних засобів ПТК ЦСК, які не задіяні в механізмах захисту і не віднесені до технологічної інформації КЗЗ.

4.1.4 Позамашинна інформаційна база складається з документів, що входять до складу ПТК ЦСК.

4.2 За режимом доступу внутрішньомашинна інформація, що циркулює в ПТК ЦСК класифікується на:

- відкриту інформація, яка потребує розмежування доступу до неї у відповідності до функціональних обов'язків, які покладені на персонал ЦСК і до якої висуваються підвищені вимоги до забезпечення цілісності й доступності інформації;
- інформація з обмеженим доступом до якої висуваються підвищені вимоги із забезпечення конфіденційності та цілісності.

4.3 У ЦСК до ІзОД відносяться:

- особисті ключі ЦСК та персоналу ЦСК;
- персональні дані зовнішніх користувачів;
- технологічна інформація КЗЗ ЦСК.

4.4 За правовим режимом інформація з обмеженим доступом в ЦСК класифікується, як конфіденційна інформація.

4.5 Вищий гриф обмеження доступу до інформації, яка обробляється в ЦСК - "конфіденційно".

5 ОПИС КОМПОНЕНТІВ ЦСК ТА ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ

5.1 Опис компонентів ЦСК та технології обробки інформації наведені у дод. 2.

6 ЗАГРОЗИ ДЛЯ ІНФОРМАЦІЇ В ЦСК

6.1 Загрози для інформації в ЦСК наведені у окремому документі - модель загроз безпеки інформації в ЦСК.

7 ОСНОВНІ ПОЛОЖЕННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ В ЦСК

7.1 Організаційні, технологічні і технічні заходи щодо захисту інформації в ЦСК повинні проводитися у відповідності до вимог чинного законодавства, нормативних і інших документів Адміністрації Держспецзв'язку України, а також нормативно-методичними матеріалами і організаційно-розпорядчими документами ДП "ЕНЕРГОРИНОК" з питань забезпечення інформаційної безпеки в ЦСК.

7.2 Всі ресурси ЦСК повинні бути встановленим порядком категорійовані (для кожного ресурсу повинен бути визначений необхідний рівень захищеності). Ресурси системи, які потребують захисту (інформація, задачі, програми, робочі станції, сервери і т.д.), підлягають обліку (на основі використання відповідних формулярів або спеціалізованих баз даних).

7.3 На всіх РС ЦСК, які підлягають захисту, повинні бути встановлені необхідні технічні засоби захисту (відповідно до рівня захищеності - категорії РС). Для користувачів захищених РС повинні бути розроблені необхідні технологічні інструкції, які включають вимоги з забезпечення інформаційної безпеки. Експлуатація в структурних підрозділах ЦСК захищених РС повинна бути дозволена тільки за наявності формулярів РС (паспортів-розпоряджень на їх експлуатацію, що свідчать про виконання всіх необхідних вимог інформаційної безпеки).

7.4 Всі співробітники ЦСК, що використовують при роботі ЦСК, повинні бути ознайомлені з планом захисту ЦСК в частині, що їх стосується, повинні знати і неухильно виконувати технологічні інструкції. Доведення вимог до осіб, допущених до обробки інформації, що захищається, повинне здійснюватися начальниками підрозділів під розпис.

7.5 Співробітники ЦСК, які допущені до роботи з ЦСК, повинні нести персональну відповідальність за порушення встановленого порядку автоматизованої обробки інформації, правил зберігання, використання і передачі ресурсів системи, які знаходяться в їх розпорядженні та потребують захисту. Кожний співробітник (при прийомі на роботу або при допуску до роботи з ресурсами ЦСК, що захищаються) повинен підписувати угоду (зобов'язання) про дотримання і відповідальність за порушення встановлених вимог по збереженню службової таємниці, а також правил роботи з ІЗОД в ЦСК. Будь-яке грубе порушення порядку і правил роботи в ЦСК співробітниками ЦСК повинне розслідуватися. До порушників повинні застосовуватися адекватні дії. Міра відповідальності персоналу за дії, які порушують встановлені правила забезпечення захищеної автоматизованої обробки інформації, визначаються завданням збитком, наявністю злого наміру і інших факторів з розсуду керівництва ЦСК.

7.6. Допуск співробітників ЦСК до роботи з ЦСК і доступ до його ресурсів повинен бути регламентований. Будь-які зміни складу і повноважень користувачів ЦСК повинні здійснюватися встановленим порядком згідно інструкції по внесенню змін в списки користувачів ЦСК і наділенням їх повноваженнями доступу до ресурсів системи.

7.7 Кожному співробітнику ЦСК (користувачу) повинні надаватися мінімально необхідні права і повноваження з доступу до ресурсів ЦСК (виробнича необхідність надання співробітникам повноважень і прав доступу до ресурсів ЦСК визначається керівництвом відповідних структурних підрозділів) для виконання функціональних обов'язків. Жоден співробітник ЦСК не повинен володіти всією повнотою повноважень для одноосібного безконтрольного знищення, зміни або створення і авторизації ресурсів в ЦСК. Керівники структурних підрозділів зобов'язані своєчасно надавати заявки на надання своїм співробітникам або позбавлення (у разі звільнення, переведення, хвороби і т.п.) співробітників відповідних прав доступу і повноважень по роботі з ресурсами ЦСК.

7.8. Апаратно-програмна конфігурація робочих станцій (автоматизованих робочих місць), на яких обробляється інформація, що захищається, повинна відповідати складу покладених на користувачів даної РС функціональних обов'язків. Всі невживані в роботі (зайві) пристрої уведення-виведення інформації на таких РС повинні бути відключені (вилучені фізично або логічно). Не потрібні для роботи програмні засоби і дані з дисків РС повинні бути вилучені.

7.9 Для спрощення супроводу, обслуговування і організації захисту РС повинні оснащуватися програмними засобами і конфігуруватися уніфіковано (відповідно до встановлених правил).

7.10 Введення в експлуатацію нових РС та серверів і всі зміни в конфігурації технічних і програмних засобів існуючих РС (серверів) в ЦСК повинні здійснюватися тільки встановленим порядком згідно інструкції по установці, модифікації і технічному обслуговуванню програмного забезпечення і апаратних засобів ЦСК.

7.11 Все програмне забезпечення (розроблене фахівцями ЦСК, отримане централізовано або закупленого у фірм виробників) повинне встановленим порядком проходити перевірку (випробування) і передаватися до архіву еталонних програм ЦСК. В ЦСК повинні встановлюватися і використовуватися тільки отримані встановленим порядком програмні засоби. Використання ПЗ, яке не поставлене на облік встановленим порядком, заборонено.

7.12 Фізична цілісність апаратних компонентів РС та серверів повинна забезпечуватися організаційними заходами із застосуванням механічних замків (за наявності), пломб (наклейок, печатки тощо) на блоках і пристроях засобів обчислювальної техніки. Повсякденний контроль за цілісністю і відповідністю печатки (пломб, наклейок) повинен здійснюватися користувачами і адміністратором безпеки ЦСК. Періодичний контроль - адміністратором безпеки або керівником СЗІ ЦСК.

7.13 Експлуатація ЦСК повинна здійснюватися в приміщеннях, обладнаних автоматичними замками, засобами сигналізації і постійно знаходитися під охороною або спостереженням, що виключає можливість безконтрольного проникнення в приміщення сторонніх осіб і забезпечує фізичне збереження ресурсів, що захищаються (РС, серверів, документів, реквізитів доступу і т.п.). Розміщення і установка технічних засобів повинна виключати можливість візуального перегляду інформації, що вводиться (виводиться), особами, які не мають до неї відношення.

7.14 Прибирання приміщень зі встановленими в них ПЕОМ повинне проводитися у присутності відповідального, за яким закріплені дані технічні засоби, або чергового по підрозділу з дотриманням заходів, що виключають доступ сторонніх осіб до ресурсів, що захищаються.

7.15 В приміщеннях під час обробки і відображення конфіденційної інформації повинні бути присутні тільки особи, які допущені до роботи з даною інформацією. Організація прийому відвідувачів повинна виключати можливість їх візуального ознайомлення з інформацією, яка потребує захисту, до якої вони не допущені.

7.16 Після закінчення робочого дня (у випадку, якщо ЦСК працює не цілодобово або перед святами) приміщення ЦСК повинні здаватися під охорону, з включенням сигналізації і відміткою в книзі прийому і здачі службових приміщень.

7.17 Розробка ПЗ задач (комплексів задач) ЦСК, проведення випробувань розробленого і придбаного ПЗ, передача ПЗ в експлуатацію повинні здійснюватися відповідно до затвердженого порядку розробки, проведення випробувань і передачі задач (комплексів задач) в експлуатацію.

7.18 Більш докладніше політика безпеки інформації наведене у окремому документі „Політика безпеки інформації”.

8 ПОЛОЖЕННЯ ПРО ЗАХИСТ ІНФОРМАЦІЇ ЦСК

8.1 Забезпечення безпеки інформації в ЦСК досягається шляхом створення комплексної системи захисту інформації (КСЗІ). Метою створення КСЗІ ЦСК є забезпечення захисту інформації, яка циркулює у ЦСК, від несанкціонованого доступу шляхом здійснення протидії загрозам, які можна очікувати внаслідок дій порушника. Захист інформації повинен забезпечуватися на всіх технологічних етапах її обробки і в усіх режимах функціонування ЦСК.

8.2 При розробці та впровадженні КСЗІ ЦСК повинні бути враховані існуючі тенденції розвитку захищених інформаційних технологій, розробки відповідних засобів захисту інформації, розвитку державної нормативної бази з технічного захисту інформації.

8.3 Для здійснення захисту інформації на всіх стадіях життєвого циклу ЦСК комплексна система захисту інформації повинна передбачати застосування наступних заходів та засобів захисту інформації:

- організаційно-правові заходи, які реалізуються поза обчислювальною системою ЦСК;
- інженерно-технічні заходи, що реалізуються поза обчислювальною системою ЦСК;
- апаратні, програмно-апаратні та програмні засоби захисту від несанкціонованого доступу до інформації, яка обробляється й зберігається в ЦСК.

Захист інформації, яка обробляється й зберігається в ЦСК, від НСД здійснюється комплексом засобів захисту (КЗЗ) ПТК ЦСК.

8.4 КСЗІ ЦСК призначена для:

- реалізації політики безпеки інформації ЦСК;
- забезпечення конфіденційності, цілісності, доступності інформації під час експлуатації ЦСК;
- недопущення витоку інформації з обмеженим доступом та втрати її матеріальних носіїв;
- створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації та оперативного оповіщення адміністраторів безпеки про факти несанкціонованого доступу до інформації;
- ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів обчислювальної системи ЦСК, причин та умов, які спричиняють або можуть привести до порушення її нормального функціонування;
- керування засобами захисту інформації, розмежування доступу користувачів до ресурсів ЦСК, контроль за їхньою роботою з боку осіб, які відповідають за забезпечення безпеки інформації в ЦСК;
- створення умов для забезпечення максимально можливого рівня локалізації негативних наслідків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення безпеки на функціонування ЦСК;
- організації обліку, зберігання, обігу інформації, яка потребує захисту, та матеріальних носіїв, на яких вона накопичується;
- реєстрації, збору, зберігання, обробки даних про всі події в ЦСК, які мають відношення до безпеки інформації;
- забезпечення доступності ресурсів ЦСК для її користувачів.

8.5 Організація робіт зі створення та супроводження КСЗІ, управління засобами захисту інформації, контроль за дотриманням положень політики безпеки здійснюється службою захисту інформації, функції якого виконує персонал ЦСК.

8.6. Політика безпеки визначає ресурси, що потребують захисту, враховує основні загрози для інформації і моделі порушників, впроваджені технології оброблення інформації і вимоги до захисту інформації від загроз.

КСЗІ повинна підтримувати коректно визначену політику безпеки - множину правил, які при заданій класифікації суб'єктів доступу і об'єктів захисту використовуються для визначення можливості надання дозволу на доступ конкретного суб'єкта до конкретного об'єкта, надання та зміни повноважень, моніторингу всіх подій, які впливають на безпеку, та їх реєстрації.

8.7 Політика безпеки, яка реалізується КСЗІ ЦСК для захисту інформації від потенційних внутрішніх та зовнішніх загроз, поширюватись на наступні об'єкти захисту:

- відомості (незалежно від виду їхнього представлення), що віднесені до інформації з обмеженим доступом (ІзОД) або інших видів інформації, що підлягають захисту, обробка яких здійснюється в ЦСК і які можуть знаходитись на паперових, магнітних, оптичних та інших носіях;
- інформаційні масиви та бази даних, програмне забезпечення, інші інформаційні ресурси;

- обладнання ЦСК та інші матеріальні ресурси, включаючи технічні засоби та системи, не задіяні в обробці ІзОД, але знаходяться у контрольованій зоні, носії інформації, процеси і технології її обробки. Технічні області, в яких необхідно захищати інформаційне та програмне забезпечення - робоча станція, комунікаційні канали (фізична мережа) та комутаційне обладнання, сервери, засоби друку, накопичувачі інформації;
- засоби та системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту;
- користувачів (персонал) ЦСК, власників інформації та ЦСК, а також їхні права.

8.8.1 КЗЗ ПТК ЦСК, що входить до складу КСЗІ ЦСК, повинен мати атестат відповідності або експертний висновок щодо його відповідності вимогам НД ТЗІ 2.5-004. За умови їх відсутності такий атестат відповідності або експертний висновок можуть бути отримані при проведенні державної експертизи КСЗІ ЦСК.

8.8.2 КСЗІ ЦСК повинна забезпечити безпеку засобів КЗІ та захист інформаційних ресурсів ЦСК від зовнішніх загроз, атак та несанкціонованого витоку інформації шляхом створення й підтримки безпечних інформаційних технологій, в рамках яких доступ до інформації різних категорій організується таким чином, що тільки уповноваженим користувачам або процесам надається можливість роботи з конкретною інформацією, доступ до якої обмежується і гарантується цілісність при її обробці, зберіганні та транспортуванні у електронному вигляді, у вигляді друкованого документу або набору даних, що містяться на змінних носіях інформації.

8.8.3 Робота ЦСК в штатних режимах повинна бути можливою лише при функціонуючій КСЗІ. У разі відмови КСЗІ (окремого її модуля, компонента) повинен передбачатись режим аварійного блокування роботи ЦСК чи окремого його компонента. Порядок дій користувачів і обслуговуючого персоналу у цих випадках визначається Планом захисту інформації ЦСК.

8.8.4 Інформаційні послуги, що їх надають компоненти ЦСК повинні надаватись тільки зареєстрованим користувачам за умови їх достовірного розпізнавання.

8.8.5 КСЗІ ЦСК повинна вести облік і здійснювати реєстрацію подій, які пов'язані із безпосереднім доступом (спробами доступу) до інформації, здійснювати періодичний контроль за такими подіями та забезпечувати захист реєстраційної інформації від несанкціонованої модифікації, руйнування або знищення. Обсяг реєстраційної інформації повинен бути достатнім для встановлення причин та джерела виникнення зареєстрованої події.

8.8.6 КСЗІ повинна унеможливити з боку користувачів несанкціоноване або неконтрольоване використання ресурсів ЦСК.

8.8.7 Критичні з точки зору безпеки компоненти КСЗІ ЦСК повинні резервуватися, з тим щоб їх відмова не призводила до переривання процесу надання послуг користувачам.

8.8.8 Організація захисту інформації в ЦСК має визначатися сукупністю нормативно-розпорядчих та технічних документів, які складають План захисту інформації ЦСК.

8.8.9 Будівлі, де розміщується ЦСК повинні бути розміщені в межах контрольованої території, що має перепускний та внутрішній режими, які відповідають режимним вимогам, що визначено чинними в ДП "ЕНЕРГОРИНОК" нормативними та розпорядчими документами.

8.8.10 Контроль за доступом до приміщень, де знаходиться обчислювальна система ПТК ЦСК, носії з копіями даних та програмного забезпечення ПТК ЦСК повинен забезпечуватись на всіх етапах його життєвого циклу. Порядок доступу до таких приміщень із визначенням категорій користувачів, які мають право це здійснювати, визначається службою захисту інформації ЦСК (далі - СЗІ) і затверджується начальником ЦСК ринку електричної енергії.

8.8.11 Користувачі ЦСК повинні мати належний рівень кваліфікації і володіти навиками для виконання робіт відповідно до покладених на них завдань. Вони повинні мати дозвіл начальника ЦСК на доступ до інформації ЦСК згідно з службовими обов'язками.

9 ПОРЯДОК ПЕРЕГЛЯДУ ПЛАНУ ЗАХИСТУ

9.1 План захисту підлягає частковому перегляду в наступних випадках:

- при зміні конфігурації, додаванні або вилученні програмних і технічних засобів в ЦСК, що не змінює технологію обробки інформації;
- при зміні конфігурації і налаштувань технічних засобів захисту, що використовуються в ЦСК;
- при зміні складу і обов'язків користувачів і обслуговуючого персоналу ЦСК і співробітників, що відповідають за інформаційну безпеку.

9.2 Профілактичний перегляд плану захисту проводиться не рідше 1 разу на рік і має на меті перевірку відповідності визначених даним планом заходів реальним умовам застосування ЦСК і поточним вимогам до його захисту.

9.3 План захисту підлягає повному перегляду у разі зміни технології обробки інформації або використанні нових технічних засобів захисту.

9.4 У разі часткового перегляду можуть бути добавлені, вилучені або змінені різні додатки до плану захисту ЦСК з обов'язковою вказівкою в листі реєстрації змін даних про те, хто, коли, з якою метою, які зміни вніс і хто санкціонував ці зміни.

9.5 Зміни, що вносяться в план, не повинні суперечити іншим положенням плану захисту і повинні бути перевірені на коректність та повноту.

9.6 Будь-який перегляд плану захисту повинен здійснюватися з обов'язковою участю представників служби захисту інформації ЦСК.

10 ВІДПОВІДАЛЬНІ ЗА РЕАЛІЗАЦІЮ ПЛАНУ ЗАХИСТУ

10.1 Відповідальність за реалізацію і дотримання вимог даного документа співробітниками, допущеними до роботи з ЦСК, покладається на начальника ЦСК, керівника СЗІ, адміністратора безпеки.

10.2 За реалізацію положень плану захисту, пов'язаних із застосуванням і адмініструванням технічних засобів захисту інформації від НСД відповідає служба захисту інформації ЦСК.

10.3 Реалізація положень плану захисту, пов'язаних з супроводом програмного забезпечення і обслуговуванням технічних засобів, покладається на уповноважених співробітників ЦСК.

10.4 Методичне керівництво і контроль за виконанням вимог цього документа покладається на службу захисту інформації ЦСК.

11 КАЛЕНДАРНИЙ ПЛАН РОБІТ З ЗАХИСТУ ІНФОРМАЦІЇ В ЦСК

11.1 Етапи життєвого циклу

11.1.1 План робіт передбачає запровадження заходів захисту на всіх етапах життєвого циклу ЦСК. Визначено такі етапи життєвого циклу ЦСК:

- створення ЦСК (включаючи створення КСЗІ) та налагодження ЦСК та КСЗІ;
- дослідна експлуатація ЦСК;
- експертиза ЦСК;
- експлуатація ЦСК (включаючи обробку ІзОД, профілактику, ремонт, модернізацію ЦСК та/або КСЗІ, тощо);
- виведення ЦСК з експлуатації.

11.1.2 Відповідно до затверджених посадових інструкцій відповідальним за організацію робіт щодо захисту ІзОД в ЦСК на всіх етапах є керівник ЦСК.

11.2 Створення КСЗІ

11.2.1 Створення КСЗІ ЦСК передбачає:

- розробку та впровадження необхідних заходів та засобів захисту відповідно до вимог НД;
- проведення попередніх випробувань КСЗІ ЦСК.

11.2.2 Після закінчення робіт щодо створення КСЗІ ЦСК з метою перевірки відповідності КСЗІ ЦСК вимогам ТЗ та НД ТЗІ проводяться попередні випробування КСЗІ.

11.2.3 Попередні випробування КСЗІ проводяться комісією, яка призначається наказом по підприємству, відповідно до затвердженої встановленим порядком програми та методик випробувань.

11.2.4 Випробування проводяться з використанням умовної інформації, яка не є ІзОД.

11.2.5 За результатами попередніх випробувань складається акт, у якому зазначаються результати випробувань і робиться висновок про можливість впровадження ЦСК (та КСЗІ) у дослідну експлуатацію.

11.3 Дослідна експлуатація

11.3.1 Автоматизована система ЦСК вводиться у дослідну експлуатацію наказом по ДП "ЕНЕРГОРИНОК" на підставі акта про проведення попередніх випробувань. В наказі зазначається відповідальний за проведення дослідної експлуатації та її термін.

11.3.2 Призначаються особи, відповідальні за експлуатацію ЦСК.

11.3.3 Відповідальність щодо забезпечення захисту ІзОД в ЦСК в процесі експлуатації покладена на керівника СЗІ.

11.3.4 Наказом по ДП "ЕНЕРГОРИНОК" створюється СЗІ, призначається керівник СЗІ, адміністратор безпеки ЦСК та системний адміністратор. Адміністратор безпеки відповідає за дотримання встановлених правил обробки ІзОД в ЦСК. Системний адміністратор відповідає за працездатність технічних та програмних засобів ЦСК.

11.3.5 Дослідна експлуатація проводиться з використанням умовної інформації, яка не є ІзОД.

11.3.6 Під час дослідної експлуатації:

- відпрацьовуються технології щодо обробки ІзОД, обігу машинних носіїв інформації, надання доступу користувачів до ресурсів ЦСК, розмежування доступу та контролю за діями користувачів;
- співробітники, які відповідають за захист ІзОД, та користувачі ЦСК набувають практичних навичок;
- здійснюється (за необхідності) доопрацювання програмного забезпечення, додаткове налагодження КЗЗ від НСД, доопрацювання інструкцій та інших документів, які входять до складу КСЗІ.

11.3.7 Після завершення дослідної експлуатації складається акт, у якому зазначаються результати дослідної експлуатації і робиться висновок про можливість пред'явлення КСЗІ на державну експертизу.

11.4 Порядок проведення державної експертизи

Державна експертиза ЦСК з ТЗІ здійснюється організатором експертизи відповідно до Положення про державну експертизу в сфері технічного захисту інформації, затвердженого наказом ДСТЗІ СБ України від 29.12.99 р. № 62.

11.5 Експлуатація

11.5.1 Автоматизована система ЦСК вводиться у промислову експлуатацію наказом по ДП "ЕНЕРГОРИНОК" на підставі атестату відповідності, отриманого від ДССЗІ України.

11.5.2 Підтримання КСЗІ ЦСК в робочому стані в процесі промислової експлуатації досягається шляхом :

- повсякденного контролю за виконанням вимог цього документу та Інструкції про порядок забезпечення режиму безпеки в ЦСК;
- постійного контролю за працездатністю комплексу засобів захисту інформації від несанкціонованого доступу.

11.5.3 Доступ співробітників ЦСК ринку електричної енергії до роботи в ЦСК надається наказом директора ДП "ЕНЕРГОРИНОК" за поданням начальника відповідного структурного підрозділу, що оформлюється у вигляді заявки.

11.5.4 Користувачі несуть відповідальність за дотримання ними встановлених правил обробки ІзОД під час роботи в ЦСК.

11.5.5 Порядок обробки ІзОД регламентується інструкціями та іншими документами, перелік яких наведено в розділі 7 даного документу.

11.6 Модернізація

11.6.1 У разі необхідності проведення модернізації ЦСК повинні бути переглянуті засоби та заходи захисту, які становлять КСЗІ ЦСК, що має бути відображено у Плані захисту.

11.6.2 Порядок дій під час модернізації ЦСК має бути аналогічним порядку, викладеному у п.п.13.2-13.4 цього документа.

11.7 Виведення з експлуатації

11.7.1 Порядок виведення ЦСК з експлуатації розробляється після прийняття рішення про припинення експлуатації.

11.7.2 У загальному випадку порядок виведення ЦСК з експлуатації повинен передбачати:

- призначення відповідального за виведення ЦСК з експлуатації;
- розроблення порядку видалення ІзОД з носіїв, які можуть використовуватися пізніше для оброблення відкритої інформації (в інших системах);
- розроблення порядку переносу ІзОД у інші системи (у разі необхідності).

11.7.3 Календарний план робіт з захисту інформації наведений в окремому документі.

12 СИСТЕМА ДОКУМЕНТІВ З ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЦСК

12.1 Порядок обробки та захисту інформації в ЦСК регламентується нормативними документами, зазначеними в дод. 1, та такими документами:

- план захисту інформації в ЦСК (цей документ);
- інструкція про порядок забезпечення режиму безпеки в ЦСК;
- інструкції та інші експлуатаційні документи із складу матеріалів техноробочого проекту ЦСК;
- розпорядження, накази та інші організаційно-розпорядчі документи ДП "ЕНЕРГОРИНОК".

12.2 Проектна та експлуатаційна документація на компоненти КСЗІ має містити основні проектні рішення щодо побудови захисту ЦСК, опис компонентів КСЗІ, основні правила її експлуатації.

12.3 Опис КСЗІ містить відомості про склад КСЗІ, функціонування механізмів захисту, способи реалізації послуг безпеки та ін.

12.4 Документація техноробочого проекту повинна містити основні проектні і технічні рішення щодо побудови КСЗІ (компонентів КСЗІ). Склад та зміст документації повинен відповідати наступним вимогам:

- в частині виготовлення конструкторської документації - стандартам ЄСКД;
- в частині виготовлення програмної документації - стандартам ЄСПД;
- в частині виготовлення експлуатаційної документації - ГОСТ 34.201, РД 50-34.698.

Остаточний склад експлуатаційної документації уточнюється на стадії техноробочого проекту.

12.5 У разі потреби розробляються інші документи з забезпечення захисту інформації.

13 ПОРЯДОК ДІЙ У РАЗІ ВІДМОВИ КСЗІ ЧИ ОКРЕМОГО КОМПОНЕНТА

13.1 Компонентами КСЗІ є КЗЗ операційних систем та КЗЗ зі складу програмно-технічного комплексу ЦСК.

13.2 У випадку виходу з ладу КЗЗ ОС:

- користувач повинен звернутися до адміністратора безпеки;
- дії адміністратора безпеки в цьому випадку залежать від діагностичних повідомлень операційної системи;
- у разі незворотної помилки необхідно виконати повторну інсталяцію операційної системи.

13.3 У випадку порушення цілісності носіїв з ключовою інформацією, вони повинні бути замінені у встановленому порядку.

13.4 У випадку виходу з ладу апаратно-програмного компоненту зі складу ПТК (порушення цілісності, невиконання процесу самотестування та інше) порядок дій визначається експлуатаційною документацією на ПТК.

14 ВИКОНАННЯ РОБІТ, ПОВ'ЯЗАНИХ З ТЕХНІЧНИМ ОБСЛУГОВУВАННЯМ

14.1 Порядок виконання робіт, пов'язаних з регламентним технічним обслуговуванням компонентів ЦСК, визначений адміністраторами відповідних компонентів ЦСК за погодженням з адміністратором безпеки і наведений у інструкціях з експлуатації ПТК.

ДОДАТОК 1. ПЕРЕЛІК НОРМАТИВНИХ, РОЗПОРЯДЧИХ, ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ ТА ІНШИХ ДОКУМЕНТІВ, ЗГІДНО З ЯКИМИ ПОВИНЕН ЗДІЙСНЮВАТИСЯ ЗАХИСТ ІНФОРМАЦІЇ В ЦСК

- Закон України „Про інформацію”;
- Закон України „Про захист інформації в інформаційно-телекомунікаційних системах”;
- Закон України „Про електронний цифровий підпис”;
- Концепція технічного захисту інформації в Україні. Затверджена Постановою Кабінету Міністрів України від 8.10.97 №1126;
- Положення про технічний захист інформації в Україні. Затверджене Указом Президента України від 27.09.99 № 1229/99;
- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;
- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення;
- ДСТУ 3918-99. Інформаційні технології. Процеси життєвого циклу програмного забезпечення;
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22;
- НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ від 28 квітня 1999 року №22;
- НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджений наказом ДСТСЗІ СБУ №37 від 18.06.2002 р.;
- НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджений наказом ДСТСЗІ СБУ від 4 грудня 2000 року №53;
- НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ від 28 квітня 1999 року №22;
- НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ від 28 квітня 1999 року №22;
- НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджений наказом ДСТСЗІ СБУ від 13.12.2002 р. №84;
- НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджений наказом ДСТСЗІ СБУ від 20 грудня 2000 року №60;
- НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджений наказом ДСТСЗІ СБУ від 09.02.2001 №2
- Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом ДСТСЗІ СБУ від 29 грудня 1999 року №62. Зареєстровано в Міністерстві Юстиції України 24 січня 2000 року за №40/4261;
- Положення про державну експертизу у сфері криптографічного захисту інформації (введене в дію Наказом ДСТСЗІ від 25.12.2000 р. № 62);
- Правила посиленої сертифікації. Затверджені наказом ДСТСЗІ СБ України від 13 січня 2005 р. № 3.

ДОДАТОК 2. ОПИС КОМПОНЕНТІВ ЦСК ТА ТЕХНОЛОГІЇ ОБРОБКИ ІНФОРМАЦІЇ

1 Функції, що їх виконує ЦСК

1.1 Центр сертифікації ключів (ЦСК) повинен забезпечити реалізацію регламентних процедур та механізмів, пов'язаних з:

обслуговуванням сертифікатів відкритих ключів (далі - сертифікатів) користувачів, що включає:

- реєстрацію користувачів;
- сертифікацію відкритих ключів користувачів;
- розповсюдження сертифікатів;
- управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів;
- надання послуг фіксування часу;

надання користувачам:

- засобів ЕЦП та шифрування даних;
- засобів генерації особистих і відкритих ключів;
- генерацію відкритих та особистих ключів користувачів усіх категорій.

1.2 Функції зазначені у п. 1.1 реалізуються програмно-технічним комплексом центру сертифікації ключів (ПТК ЦСК).

2 Обчислювальна система ЦСК

Структура та склад обчислювальної системи, програмного та програмно-апаратного забезпечення визначається особливостями ПТК ЦСК, що використовується у складі центру сертифікації ключів. Обчислювальна система ПТК ЦСК повинна відповідати вимогам, що містяться в правилах посиленої сертифікації.

2.1 До складу ПТК ЦСК повинні входити такі технічні засоби:

- центральні сервери ЦСК;
- сервери взаємодії;
- сервер моніторингу та синхронізації часу;
- комунікаційне обладнання (комутатори ЛОМ, комутатор РС, МЕ);
- РС адміністратора безпеки;
- РС адміністратора сертифікації та системного адміністратора;
- РС адміністратора реєстрації;
- РС генерації ключів користувачів.

Структурна схема комплексу технічних засобів наведена на рис. 2.1.

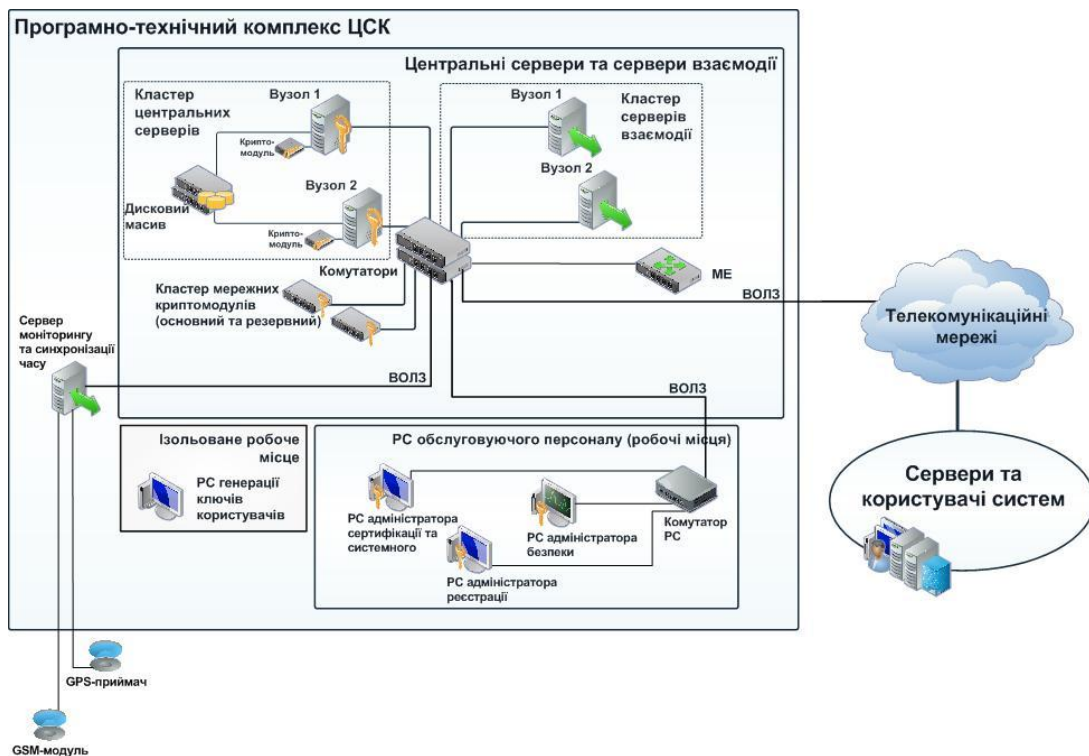


Рисунок 2.1 - Структурна схема комплексу технічних засобів.

2.2 ПТК ЦСК розгорнений як розподілена інформаційно-телекомунікаційна система, яка складається з наступних сегментів:

- серверний сегмент у складі:
 - центральні сервери ЦСК;
 - сервери взаємодії;
 - комунікаційне обладнання (комутатори ЛОМ, комутатор PC, ME);
- PC персоналу у складі:
 - PC адміністратора безпеки;
 - PC адміністратора сертифікації та системного адміністратора;
 - PC адміністратора реєстрації;
 - PC генерації ключів користувачів;

PC персоналу взаємодіють з серверним сегментом по відкритим каналам зв'язку. З серверним сегментом також взаємодіють ІТС зовнішніх користувачів ЦСК.

Центральні сервери ЦСК(БД, CMP, TSP, OCSP) реалізують основні функції з формування сертифікатів відкритих ключів користувачів ЦСК та ведення БД реєстрів користувачів та сертифікатів. БД містить як інформацію про діючі сертифікати, так і про ті, що були відкликані, а також інформацію, яка призвела до такого відкликання.

Для зберігання й застосовування особистого ключа ПТК ЦСК центральні сервери містять у своєму складі спеціалізований апаратно-програмний криптомодуль підпису.

Сервери взаємодії в складі ПТК ЦСК забезпечують у відповідності до визначених правил розмежування доступу коректну взаємодію як локальних, так і віддалених адміністраторів реєстрації, а також користувачів ЦСК і взагалі будь-яких інших користувачів, що намагаються отримати доступ до ЦСК.

Іншою функцією серверу взаємодії є забезпечення підтримки електронного інформаційного ресурсу ЦСК - загальнодоступних каталогів (LDAP-каталоги) та web-сторінки ЦСК, що містить загальнодоступну інформацію про сертифікати відкритих ключів користувачів ЦСК, списки відкликаних сертифікатів тощо.

З кожними із зазначених серверів взаємодіють PC адміністраторів, з яких здійснюється ініціалізація функціональних задач ЦСК. PC використовуються адміністратором безпеки, системним адміністратором, адміністратором реєстрації.

Для об'єднання серверів в єдину локальну мережу застосовуються комутаційні пристрої.

2.3 Взаємодія локальної мережі ПТК ЦСК із зовнішніми телекомунікаційними мережами здійснюється через міжмережевий екран (МЕ).

МЕ призначений для:

- забезпечення захисту ПТК ЦСК від зовнішніх атак;
- забезпечення захисту ПТК ЦСК від несанкціонованих дій персоналу ЦСК.
- МЕ повинен забезпечувати:
 - контроль транзитної інформації протоколів прикладного рівня;
 - захист від мережевих атак, таких як, відмова в обслуговуванні, атака фрагментами та інших, що можуть здійснюватися із зовнішньої телекомунікаційної мережі;
 - трансляцію IP-адресів та портів протоколів транспортного рівня;
 - перевірку та висліджування стану всіх мережевих з'єднань;
 - фільтрацію пакетів на підставі списків контролю доступу (на основі MAC-адреси або IP-адреси, номеру TCP- або UDP-порта відправника/приймальника);
 - захист від витоку за межі ЦСК ключів обслуговуючого персоналу ЦСК особистої інформації про користувачів ЦСК.

Управління МЕ повинне здійснюватися:

- з локальної консолі, яка підключається безпосередньо до консольного порту комутатора;
- з РС адміністратора безпеки з використанням засобів адміністрування МЕ та його КЗЗ.

Управління з локальної консолі повинне застосовуватися при первинному налагодженні та в аварійних ситуаціях з використанням командного інтерфейсу ОС МЕ.

МЕ повинен розміщуватися у шафі разом з сервером взаємодії та комутатором ЛОМ.

2.4 Окремим компонентом ПТК ЦСК, що не підключений до локальної мережі і працює в автономному режимі є РС генерації ключів користувачів.

2.5 Для здійснення криптографічних перетворень використовуються спеціалізовані апаратно-програмні модулі підпису, які мають експертний висновок ДССЗІ України.

2.6 Склад системного програмного забезпечення ЦСК

2.6.1 Системне програмне забезпечення включає наступні основні компоненти:

- операційна система Microsoft Windows 8.1 Enterprise для робочих станцій;
- операційні системи серверів Microsoft Windows 2012 Server R2 Standard, FreeBSD;
- системи керування базами даних - MS SQL Server, MySQL;
- програмні пакети, що реалізують служби взаємодії із зовнішньою телекомунікаційною мережею - OpenLDAP, Apache, Exim.

2.6.2 Системне ПЗ ПТК ЦСК повинне забезпечувати виконання наступних основних функцій:

- колективну роботу користувачів;
- адміністрування компонентів ПТК ЦСК;
- збереження структурованої і неструктурованої інформації ПТК ЦСК;
- доступ до файлів, баз даних і електронних документів колективного користування ЦСК;
- обмін даними між компонентами ЦСК і користувачами зовнішньої телекомунікаційної мережі.

2.6.3 Системне ПЗ повинно мати ліцензію та використовуватися із дотриманням ліцензійних умов виробника ПЗ, встановлюватися та оновлюватися з урахуванням практичних рекомендацій виробника ПЗ.

3 Особливості функціонування ЦСК

3.1 ЦСК повинен функціонувати безперервно цілодобово окрім режиму технічного обслуговування. Виконання робіт, пов'язаних з регламентним технічним обслуговуванням компонентів ЦСК, здійснюється у порядку, визначеному адміністраторами відповідних компонентів ЦСК за погодженням з адміністратором безпеки та включається до Плану захисту ЦСК.

3.2 В якості носіїв ключової інформації повинні використовуватися:

- з'ємні диски (гнучкі диски 3,5", електронні диски із внутрішнім ПЗП);
- компакт-диски (CD-R, CD-RW, DVD-R або DVD-RW);
- електронні ключі "ІІТ.Кристал", Aladdin eToken R2, PRO та інші.

4 Середовище користувачів

За рівнем повноважень відповідно до характеру та складу робіт, які виконуються в процесі функціонування ЦСК, користувачі та обслуговуючий персонал (далі - користувачі), що мають доступ до нього, поділяються на такі категорії:

- 1) персонал ЦСК, який має повноваження супроводжувати КЗЗ ПТК ЦСК (виконує функції адміністратора безпеки);
- 2) персонал ЦСК, який має повноваження інших адміністраторів (системного адміністратора ПТК);
- 3) персонал ЦСК, який має повноваження здійснювати функції з обробки інформації ПТК ЦСК, здійснювати обмін службовими повідомленнями з відокремлених робочих станцій реєстрації та забезпечує підтримку загальнодоступних каталогів (LDAP-каталоги) та інформаційних ресурсів ЦСК (web-сторінка) (адміністратори реєстрації (у тому числі відокремлені));
- 4) технічний обслуговуючий персонал, що забезпечує належні умови функціонування ЦСК, повсякденне підтримання життєдіяльності фізичного середовища ЦСК тощо;
- 5) постачальники, розробники та проектувальники апаратних засобів та функціонального програмного забезпечення ПТК ЦСК, що забезпечують їх модернізацію, супроводження та розвиток;
- 6) абоненти ЦСК - суб'єкти господарської діяльності, що отримали або реалізують процедуру отримання сертифіката відкритих ключів і надають до ЦСК необхідну для інформацію;
- 7) абоненти мереж загального користування - будь-які особи, що мають доступ до зовнішніх телекомунікаційних мереж (наприклад, Internet) та намагаються отримати доступ до Web-сторінки та /або загальнодоступних каталогів ЦСК.

5 Умови розташування об'єкту

Об'єкти, на яких розгорнуті компоненти ПТК ЦСК, повинні бути розташовані в приміщеннях, що відповідають експлуатаційним вимогам до компонентів ПТК ЦСК, вимогам, що сформульовані у Правилах посиленої сертифікації.